Osamu Kawamura et al
82478-0100
JW Price
949-253-4820

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年 ８月２７日

出願番号
Application Number: 特願２００２－２４７６９３

[ST.10/C]: [ＪＰ２００２－２４７６９３]

出願人
Applicant(s): 松下電器産業株式会社

２００３年 ５月 ９日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号 出証特２００３－３０３３６１１

【書類名】　特許願

【整理番号】　2022540038

【提出日】　平成14年 8月27日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C　1/00

H04L　9/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　河村　領

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　尾坂　匡隆

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9003742

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　並列ストリーム暗復号装置及びその方法並びに並列ストリーム暗復号プログラム

【特許請求の範囲】

【請求項１】　ストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路と、

入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理手段と、

出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算手段とを備えることを特徴とする並列ストリーム暗復号装置。

【請求項２】　前記入力ストリーム処理手段は、クロスバスイッチを有し、ストリームデータの入力線とストリームデータを暗号化又は復号化する鍵に対応する経路に接続される出力線との接点のスイッチをオンに設定することにより、対応する経路にストリームデータを出力することを特徴とする請求項１記載の並列ストリーム暗復号装置。

【請求項３】　前記暗復号演算手段で暗号化又は復号化された複数のストリームデータの入力を受け、複数の出力インターフェースに各暗号化又は復号化されたストリームデータをそれぞれ出力する出力ストリーム処理手段を更に備えることを特徴とする請求項１記載の並列ストリーム暗復号装置。

【請求項４】　前記出力ストリーム処理手段は、クロスバスイッチを有し、

前記出力ストリーム処理手段から出力される複数の暗号化又は復号化されたストリームデータの出力先の出力インターフェースを前記経路に応じてクロスバスイッチをオンオフ制御して切り換える制御手段と、

複数の経路へ出力されたストリームデータと対応する鍵とを前記暗復号演算手段に経路毎に入力し、入力したストリームデータの経路情報を前記制御手段に通知する入力通知手段を更に備えることを特徴とする請求項３記載の並列ストリーム暗復号装置。

【請求項５】　前記暗復号演算手段を複数備え、

前記複数の経路へ出力されるストリームデータと対応する鍵とを各暗復号演算

手段に並列入力し、各暗復号演算手段に入力したストリームデータの経路情報を通知する入力通知手段と、

前記経路情報に従い、前記出力ストリーム処理手段から出力される複数の暗号化又は復号化されたストリームデータの出力先の出力インターフェースを選択制御する制御手段とを更に備えることを特徴とする請求項３記載の並列ストリーム暗復号装置。

【請求項６】　前記暗復号演算手段から出力された暗号化又は復号化されたストリームデータを再度前記入力ストリーム処理手段に入力する経路を更に備え、

前記暗復号演算手段は、暗号化又は復号化されたストリームデータを異なる鍵で暗号化又は復号化することを特徴とする請求項１記載の並列ストリーム暗復号装置。

【請求項７】　前記入力ストリーム処理手段は、入力される複数のストリームデータをマルチプレクス処理して１つのストリームデータを生成することを特徴とする請求項１記載の並列ストリーム暗復号装置。

【請求項８】　前記入力ストリーム処理手段は、入力される１つのストリームデータをデマルチプレクス処理して複数のストリームデータを生成することを特徴とする請求項１記載の並列ストリーム暗復号装置。

【請求項９】　前記入力ストリーム処理手段は、入力される１つのストリームデータを２つの経路に出力し、

１つの経路は、前記暗復号演算手段に、別の経路は、直接前記出力ストリーム処理手段にそれぞれ接続されていることを特徴とする請求項３記載の並列ストリーム暗復号装置。

【請求項１０】　ストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路を備える並列ストリーム暗復号装置における並列ストリーム暗復号方法であって、

入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理ステップと、

出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算

ステップとを有することを特徴とする並列ストリーム暗復号方法。

【請求項１１】　請求項１０記載の並列ストリーム暗復号方法をコンピュータに実行させるプログラム。

【請求項１２】　請求項１記載の並列ストリーム暗復号装置を組み込んだＴＶ受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、受信した番組を記録する記録装置を有するＴＶ受信装置に組み込まれる複数のストリームデータを並列に暗号化、復号化する並列ストリーム暗復号装置に関する。

【０００２】

【従来の技術】

最近、ＴＶ受信装置は、放送局から放送される放送番組を受信して放映するだけでなく、例えば、インターネットのブロードバンド放送の番組を通信回線を経由して受信して放映したり、受信した番組を例えばＨＤＤに蓄積し、後で視聴できるようにと種々の形態で使用されている。また、市販のＤＶＤ（デジタル多目的ディスク）等のコンテンツの再生もＴＶ受信装置を利用して行われている。

【０００３】

これらの放送番組等のコンテンツは、著作権保護等を目的として暗号化されて放送されているので、復号化する必要がある。また、一旦復号化したコンテンツを記録媒体に記録するとき、再度暗号化を施す場合がある。

図１６は、ＴＶ受信装置に組み込まれた従来の並列ストリーム暗復号装置の構成図である。

【０００４】

この並列ストリーム暗復号装置は、入力インターフェース１６０１～１６０５と、ストリーム解析部１６１０と、制御部１６１１と、ストリーム処理部１６２１と、鍵１６３１～１６３４と、セレクタ１６３５と、転送調停部１６５１と、暗復号演算部１６６１と、セレクタ１６７１と、出力インターフェース１６８１

～１６８５とを備えている。

【０００５】

例えば、視聴番組のストリームデータを入力インターフェース１６０１から、録画番組のストリームデータを入力インターフェース１６０２からそれぞれ入力し、これらの暗号化されたストリームデータを暗復号演算部１６６１で復号して、復号したストリームデータを視聴番組は出力インターフェースは１６８１から、録画番組は出力インターフェース１６８２からそれぞれ出力する場合について説明する。

【０００６】

視聴番組の復号のための復号鍵を鍵１６３１に設定し、録画番組の復号のための復号鍵を鍵１６３２に設定する。

ストリーム解析部１６１０は、入力インターフェース１６０１、１６０２からそれぞれ入力されるストリームデータのパケットからヘッダ情報を抽出し、当該パケットのＰＩＤが視聴番組又は録画場組のＰＩＤと一致するか否かを制御部１６１１に通知する。制御部１６１１は、一致するときには、ストリーム処理部１６２１に当該パケットを出力するよう入力インターフェース１６０１、１６０２に指示し、一致しないときには、廃棄するよう指示する。また、制御部１６１１は、ストリーム処理部１６２１に入力インターフェース１６０１、１６０２のいずれのパケットの処理であるかを通知する。

【０００７】

入力ストリーム処理部１６２１は、入力されたパケットのフォーマットを変換し、暗復号演算部１６６１に出力する。この際、転送調停部１６５１に入力インターフェース１６０１、１６０２の何れからのデータであるかを通知する。

転送調停部１６５１は、ストリーム処理部１６２１から暗復号演算部１６６１に出力したデータが入力インターフェース１６０１のものであるときには、復号鍵１６３１を暗復号演算部１６６１に通知するようセレクタ１６３５に指示する。出力したデータが入力インターフェース１６０２のものであるときには、復号鍵１６３２を暗復号演算部１６６１に通知するようセレクタ１６３５に指示する。

【０００８】

暗復号演算部１６６１は、ストリーム処理部１６２１から入力されるデータをセレクタ１６３５から通知される復号鍵１６３１又は、復号鍵１６３２で復号化する。復号化が完了すると復号化したデータをセレクタ１６７１に出力するとともに、転送調停部１６５１に通知する。

転送調停部１６５１は、復号化されたデータを出力インターフェース１６８１又は出力インターフェース１６８２のいずれに出力するかをセレクタ１６７１に指示する。セレクタ１６７１は、暗復号演算部１６６１から入力された復号化されたデータを転送調停部１６５１から指示された出力インターフェース１６８１、１６８２にそれぞれ出力する。

【０００９】

【発明が解決しようとする課題】

ところで、上記従来の並列ストリーム暗復号装置では、暗復号演算部１６６１でデータの復号化の際に、復号鍵１６３１、１６３２をセレクタ１６３５でストリーム処理部１６２１からのデータ入力毎に選択しなければならない。

このセレクタ１６３５での復号鍵１６３１、１６３２の選択のための制御手順は複雑である。

【００１０】

本発明は、上記課題に鑑みなされたものであり、鍵選択の煩雑さを回避して並列入力されるストリームデータの暗復号のスループットの向上された並列ストリーム暗復号装置及びその方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】

上記課題を解決するため、本発明はストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路と、入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理手段と、出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算手段とを備えることとしている。

【００１２】

【発明の実施の形態】

以下、本発明に係る並列ストリーム暗復号装置の実施の形態について、図面を用いて説明する。

（実施の形態１）

図１は、本発明に係る並列ストリーム暗復号装置の実施の形態１の構成図である。

【００１３】

この並列ストリーム暗復号装置は、入力インターフェース１０１～１０５と、ストリーム解析部１１０と、ストリーム制御部１１１と、入力ストリーム処理部１２１と、調停部１５１と、暗復号演算部１６１と、出力ストリーム処理部１７１と、出力インターフェース１８１～１８５とを備え、入力ストリーム処理部１２１と調停部１５１間には、鍵１３１～１３４にそれぞれ対応付けられた経路１４１～１４４が設けられている。

【００１４】

なお、この並列ストリーム暗復号装置はＴＶ受信装置に組み込まれている。

入力インターフェース１０１～１０５は、アンテナ、外部装置、ＣＡＴＶ回線、公衆回線網とそれぞれ接続され、入力されるストリームデータをストリーム解析部１１０に通知し、ストリーム制御部１１１からの出力指示に従い、入力ストリーム処理部１２１にストリームデータを出力する。

【００１５】

例えば、入力インターフェース１０１は、アンテナに接続され、ＴＶ放送の番組のストリームデータの入力を受け、番組視聴用に出力する。入力インターフェース１０２は、同様にＴＶ放送の番組のストリームデータの入力を受け、番組録画用に出力する。入力インターフェース１０３は、ＤＶＤドライブ装置に接続され、ＤＶＤに記録されたストリームデータの入力を受け、出力する。入力インターフェース１０４は、ＣＡＴＶ回線に接続され、入力されるストリームデータを出力する。入力インターフェース１０５は、公衆回線網に接続され、インターネット放送によるストリームデータの入力を受け、出力する。

【００１６】

なお、入力インターフェース１０１～１０５の接続先は、適宜変更されて実施される。

ＴＶ受信装置において、視聴者が視聴したい番組と録画したい番組とをチャネルを選択して指定したとき、ＴＶ受信装置の制御部（図示せず）は、入力インターフェース１０１に視聴番組のトランスポートストリーム（ＴＳ）を、入力インターフェース１０２に録画番組のＴＳを入力するよう、アンテナ等を設定するとともに、ストリーム解析部１１０に視聴番組と録画番組とのＴＳパケットのＰＩＤ（パケット識別子）を通知し、鍵１３１に暗号化された視聴番組を復号する復号鍵を設定し、鍵１３２に暗号化された録画番組を復号する復号鍵を設定する。更に、ストリーム制御部１１１に入力インターフェース１０１からのデータを経路１４１に、入力インターフェース１０２からのデータを経路１４２に出力するよう指示する。また、ストリーム制御部１１１に、出力ストリーム処理部１７１において経路１４１を経由した復号化されたデータを出力インターフェース１８１に、経路１４２を経由した復号化されたデータを出力インターフェース１８２にそれぞれ出力するように指示する。

【００１７】

入力インターフェース１０１は、視聴番組のＴＳの入力を受けると、ＴＳパケットを抽出し、そのうちのヘッダ情報をストリーム解析部１１０に通知する。

ストリーム制御部１１１から出力指示を受けると抽出したＴＳパケットを入力ストリーム処理部１２１に出力する。また、廃棄指示を受けると抽出したＴＳパケットを廃棄する。

【００１８】

入力インターフェース１０２は、録画番組のＴＳの入力を受けると、ＴＳパケットを抽出し、ヘッダ情報をストリーム解析部１１０に通知する。

ストリーム制御部１１１から出力指示を受けると抽出したＴＳパケットを入力ストリーム処理部１２１に出力する。また、廃棄指示を受けると抽出したＴＳパケットを廃棄する。

【００１９】

ストリーム解析部１１０は、ＴＶ受信装置の制御部から入力インターフェース

１０１と入力インターフェース１０２とにそれぞれ入力されるＴＳから抽出すべきＴＳパケットのＰＩＤの通知を受ける。

ストリーム解析部１１０は、入力インターフェース１０１と入力インターフェース１０２とからそれぞれＴＳパケットのヘッダ情報の通知を受けると、ヘッダ情報に含まれるＰＩＤがＴＶ受信装置の制御部から通知されているそれぞれのＰＩＤと一致するか否かを判定し、その結果をストリーム制御部１１１に通知する。

【００２０】

ストリーム制御部１１１は、ＴＶ受信装置の制御部から入力インターフェース１０１からのデータを経路１４１に、入力インターフェース１０２からのデータを経路１４２に出力するよう指示され、出力ストリーム処理部２１６に経路１４１を経由した復号化されたデータを出力インターフェース１８１に、経路１４２を経由した復号化されたデータを出力インターフェース１８２にそれぞれ出力するように指示される。

【００２１】

また、ストリーム制御部１１１は、ストリーム解析部１１０からＴＳパケットのヘッダ情報の解析結果、即ち、所望のＰＩＤを有するＴＳパケットか否かの通知を受けると、ＰＩＤが一致するときには、入力インターフェース１０１、入力インターフェース１０２に入力ストリーム処理部１２１に当該ＴＳパケットを出力するようそれぞれ指示する。またＰＩＤが一致しないときには、当該ＴＳパケットを廃棄するようそれぞれ指示する。

【００２２】

ストリーム制御部１１１は、前述したＴＶ受信装置の制御部からの経路１４１、１４２への出力指示に応じて入力ストリーム処理部１２１が有するクロスバスイッチのオン、オフを設定する。

図２は、入力ストリーム処理部１２１のクロスバスイッチを示している。クロスバスイッチ２０１の入力線２０２と出力線２０３との接点の　印で示すスイッチ２０４，２０５をオンにする。○印はオフを示している。これによって、入力インターフェース１０１からのデータは経路１４１に、入力インターフェース１

０２からのデータは経路１４２にそれぞれ出力されるようになる。

【００２３】

ストリーム制御部１１１は、調停部１５１から暗復号演算部１６１に出力したデータが経路１４１又は経路１４２のいずれの経路からのデータであるかの通知を受ける。通知された経路１４１又は経路１４２に応じて出力ストリーム処理部１７１が有するクロスバスイッチのオン、オフを設定してデータの出力先の出力インターフェース１８１～１８５を切り換える。

【００２４】

入力ストリーム処理部１２１は、入力インターフェース１０１，１０２からそれぞれＴＳパケットの入力を受けると、伝送用のストリーム形式からコンテンツデータとして利用可能な形式に変換する。例えば、ＰＥＳ（パケッタイズド・エレメンタリー・ストリーム）パケットにフォーマットを変換する。変換したＰＥＳパケットは、暗号化データを復号するため設定された復号鍵１３１、１３２に対応する経路に出力する。

【００２５】

図２に示したように、入力ストリーム処理部１２１が有するクロスバスイッチ２０１のスイッチ２０４、２０５がオンにされている。これによって、視聴番組のＰＥＳパケットを復号鍵１３１に対応する経路１４１に出力し、録画番組のＰＥＳパケットを復号鍵１３２に対応する経路１４２に出力する。

鍵１３１～１３４は、レジスタで構成され、ＴＶ受信装置の制御部により、視聴者のチャネル選択に応じた番組の復号鍵がそれぞれ設定される。

【００２６】

調停部１５１は、経路１４１と経路１４２とからそれぞれ、視聴番組のＰＥＳパケットと録画番組のＰＥＳパケットの入力を受ける。視聴番組のＰＥＳパケットの入力を受けたときは、視聴番組の復号鍵１３１とともに暗復号演算部１６１に出力する。同様に、録画番組のＰＥＳパケットの入力を受けたときは、録画番組の復号鍵１３２とともに暗復号演算部１６１に出力する。

【００２７】

なお、本実施の形態では、ストリームの区切り（パケット）を復号単位として

いるので、ＰＥＳパケット単位で暗復号演算部１６１に出力するようにしたけれども、ブロック暗復号の場合には、暗復号演算単位で出力する。例えば、ＤＥＳ暗号のときには、８バイト単位でデータを出力する。

また、調停部１５１は、暗復号演算部１６１にデータを出力したとき、いずれの経路から入力されたデータであるのかをストリーム制御部１１１に通知する。

【００２８】

また、経路１４１と経路１４２とから同時にＰＥＳパケットの入力を受けたときには、例えば、経路１４１のデータを優先して暗復号演算部１６１に出力する。これは、視聴番組の方が録画番組よりもリアルタイム性が優先されることによる。全ての経路１４１～１４４からデータが入力されているときには、例えば、もっとも長い間出力されていない経路のデータを最優先して出力するようにしてもよい。なお、どのようなルールで暗復号演算部１６１にデータを出力するかは、予めＴＶ受信装置の制御部により設定されるものとする。

【００２９】

暗復号演算部１６１は、入力されるデータに暗号化又は復号化の演算を行い暗号化データ又は復号化データを出力ストリーム処理部１７１に出力する。

暗復号演算部１６１は、調停部１５１から復号鍵１３１とＰＥＳパケットとの入力又は復号鍵１３２とＰＥＳパケットとの入力を受けると、それぞれの復号鍵１３１又は復号鍵１３２を用いてＰＥＳパケットのデータを復号化する。復号化したＰＥＳパケットのデータを出力ストリーム処理部１７１に出力する。

【００３０】

出力ストリーム処理部１７１は、クロスバスイッチを有し、暗復号演算部１６１で暗号化又は復号化されたデータの入力を受け、フラグ情報等の制御情報を変換して所定の出力インターフェースに出力する。

図３、図４は、出力ストリーム処理部１７１でのクロスバスイッチの状態を説明する図である。

【００３１】

図３では、クロスバスイッチ３０１の入力線３０２と出力線３０３との接点３０４がスイッチオンの状態となっている。これは、調停部１５１からストリーム

制御部１１１に経路１４１からのＰＥＳパケットのデータ出力をしたことが通知され、ストリーム制御部１１１が、接点３０４のスイッチをオンにしたことによる。これによって、入力インターフェース１０１から入力されたＴＳデータは復号化されて出力インターフェース１８１から出力される。

【００３２】

出力ストリーム処理部１７１は、入力されたデータが暗復号演算部１６１で復号されているので、例えば、ＰＥＳ中の「スクランブルがかかっている」というフラグを「スクランブルがかかっていない」というフラグに変更する。また、ストリーム中に番組情報一覧が含まれるときに、入力インターフェース部１０１でＰＩＤが一致しないとして廃棄されたパケットデータに関する情報を削除する。

【００３３】

図４は、調停部１５１からストリーム制御部１１１に経路１４２からのＰＥＳパケットのデータ出力をしたことが通知され、ストリーム制御部１１１がクロスバスイッチ３０１の接点３０４のスイッチをオフにし、接点４０１のスイッチをオンにした状態を示している。

暗復号演算部１０１から入力された復号化されたＰＥＳデータは、入力線３０２から出力線３０３を介して出力インターフェース１８２に出力される。この際、ＰＥＳデータのフラグが「スクランブルがかかっていない」に変更されるとともに、番組情報中の削除された番組についての番組情報の変更処理がなされる。

【００３４】

出力インターフェース１８１は、ＴＶ受信装置の表示部（図示せず）に接続され、出力ストリーム処理部１７１から入力された復号化されたデータを表示部に出力し、ＴＶ番組を放映させる。

出力インターフェース１８２は、ＴＶ受信装置が内蔵するＨＤＤで構成される録画部（図示せず）に接続され、出力ストリーム処理部１７１から入力された復号化されたデータを録画部に出力し、ＴＶ番組を録画させる。

【００３５】

次に、本実施の形態の動作を図５に示すフローチャートを用いて説明する。

ＴＶ受信装置の制御部は、ユーザからの視聴番組と録画番組とのチャネル指定

に応じて、入力インターフェース１０１～１０５、出力インターフェース１８１～１８５を選択し、入力インターフェース１０１～１０５での抽出すべきＴＳパケットのＰＩＤをストリーム解析部１１０に通知し、鍵１３１から１３４に視聴番組と録画番組との復号鍵をそれぞれ設定する。また、ストリーム制御部１１１に鍵１３１～１３４のいずれに視聴番組と録画番組との復号鍵を設定したかを通知する（Ｓ５０２）。

【００３６】

選択された入力インターフェース１０１、１０２は、それぞれＴＳデータの入力を待ち（Ｓ５０４）、ＴＳパケットを抽出し、ヘッダ情報をストリーム解析部１１０に通知する（Ｓ５０６）。

ストリーム解析部１１０は、入力インターフェース１０１、１０２にそれぞれ設定されたＰＩＤと一致するＴＳパケットが入力されたか否かを判定する（Ｓ５０８）。ストリーム解析部１１０は、判定結果をストリーム制御部１１１に通知する。

【００３７】

ストリーム制御部１１１は、判定結果が一致しないときは、入力インターフェース部１０１、１０２に一致しないＴＳパケットの廃棄を指示し、Ｓ５０４に戻る。一致するときには、入力インターフェース部１０１、１０２に入力ストリーム処理部１２１にパケットデータの出力指示をする（Ｓ５１０）。

ストリーム制御部１１１は、ＴＶ受信装置の制御部から通知された復号鍵の設定に応じて、入力ストリーム処理部１２１から調停部１５１間の経路１４１～１４４のいずれの経路を入力インターフェース１０１、１０２からのデータに使用するかを定めるため、入力ストリーム処理部１２１のクロスバスイッチ２０１のオン、オフを設定する（Ｓ５１２）。

【００３８】

入力ストリーム処理部１２１は、入力インターフェース１０１、１０２からそれぞれ入力されたパケットデータのフォーマットを変換し、例えばＰＥＳ形式に変換し（Ｓ５１４）、決定された経路１４１、１４２をそれぞれ介して調停部１５１に出力する（Ｓ５１６）。

調停部１５１は、経路１４１、１４２を介してデータが入力されると経路１４１、１４２にそれぞれ対応して設定された復号鍵と当該データとを経路１４１、１４２の優先順に暗復号演算部１６１に出力するとともに、ストリーム制御部１１１に入力経路１４１、１４２の別を通知する（Ｓ５１８）。

【００３９】

ストリーム制御部１１１は、暗復号演算部１６１に入力されるデータの経路１４１、１４２に応じて出力インターフェース１８１～１８５を決定するため、クロスバスイッチ３０１のオン、オフを設定する（Ｓ５２０）。

暗復号演算部１６１は、調停部１５１から入力された復号鍵を用いて、入力された暗号化データを復号演算処理して、復号化データを出力ストリーム処理部１７１に出力する（Ｓ５２２）。

【００４０】

出力ストリーム処理部１７１は、復号化データの制御情報等を変更して、決定された出力インターフェース１８１、１８２にそれぞれ出力する（Ｓ５２４）。

ストリーム制御部１１１は、調停部１５１から入力経路１４１、１４２の通知があるか否かを判定し（Ｓ５２６）、あるときはＳ５２０に戻り、なければ、終了指示がＴＶ受信装置の制御部から有るか否かを判定し（Ｓ５２８）、なければＳ５０４に戻り、あるときには処理を終了する。

（実施の形態２）

図６は、本発明に係る並列ストリーム暗復号装置の実施の形態２の構成図である。

【００４１】

この並列ストリーム暗復号装置は、上記実施の形態１の並列ストリーム暗復号装置の暗復号演算部１６１に替えて、第１暗復号演算部６０１と第２暗復号演算部６０２とを備え、これに応じて調停部１５１に替えて、第１調停部６０３と第２調停部６０４とを備えている。また、第１暗復号演算部６０１と出力ストリーム処理部６０７との間には経路６０５が、第２暗復号演算部６０２と出力ストリーム処理部６０７との間には経路６０６がそれぞれ設けられている。また、第１調停部６０３又は第２調停部６０４のいずれかに、鍵１３１～１３４にそれぞれ

対応する経路１４１～１４４が接続される。この経路１４１～１４４と第１調停部６０３又は第２調停部６０４との接続は、ＴＶ受信装置の制御部（図示せず）により、鍵１３１～１３４の設定とともになされる。なお、本実施の形態では、経路１４１、１４２と第１調停部６０３とが、経路１４３、１４４と第２調停部６０４とが予め接続されているものとして説明する。

【００４２】

他の構成は、上記実施の形態１とほぼ同様であるので、説明を省略し、本実施の形態固有の構成について説明する。

入力インターフェース１０１から入力ストリーム処理部１２１には、上記実施の形態１と同様、放送番組のＴＳパケットが入力される。入力インターフェース１０３から入力ストリーム処理部１２１には、ＤＶＤドライブ装置（図示せず）から入力されたプログラムストリーム（ＰＳ）パケットが入力される。

【００４３】

図７に示すように、入力ストリーム処理部１２１のクロスバスイッチ７０１の接点７０２、７０３がストリーム制御部１１１によってオン状態にされている。

入力ストリーム処理部１２１は、入力インターフェース１０１から入力されたＴＳパケットをＰＥＳに変換し、経路１４１に出力する。入力インターフェース１０３から入力されたＰＳパケットは無変換のまま、経路１４３に出力する。

【００４４】

第１調停部６０３は、経路１４１からＰＥＳ形式のデータの入力を受けると、復号鍵１３１とともに第１暗復号演算部６０１に出力する。同様に第２調停部６０４は、経路１４３からＰＳパケットのデータの入力を受けると、復号鍵１３３とともに第２暗復号演算部６０２に出力する。

第１暗復号演算部６０１は、入力されたデータを復号鍵１３１で復号し、経路６０５を介して出力ストリーム処理部６０７に出力する。

【００４５】

第２暗復号演算部６０２は、入力されたデータを復号鍵１３３で復号し、経路６０６を介して出力ストリーム処理部６０７に出力する。

図８は、出力ストリーム処理部６０７が有するクロスバスイッチ８０１の設定

状態を示している。第１暗復号演算部６０１から出力される復号化されたデータの経路６０５に接続された入力線と出力インターフェース１８１に接続される出力線との接点８０２のスイッチがストリーム制御部１１１によってオンにされている。また、第２暗復号演算部６０２から出力される復号化されたデータの経路６０６に接続された入力線と出力インターフェース１８３に接続される出力線との接点８０３のスイッチがストリーム制御部１１１によってオンにされている。これによって、第１暗復号演算部６０１で復号化された放送番組のＰＥＳ形式のデータは、出力ストリーム処理部６０７で「スクランブルがかかっていない」にフラグ変換され、出力インターフェース１８１に出力される。出力インターフェース１８１は、このデータの入力を受け、図示しないＴＶ受信装置の表示部に放送番組を出力する。

【００４６】

また、第２暗復号演算部６０２で復号化されたＤＶＤに記録されたＰＳのデータは、出力ストリーム処理部６０７で「暗号化されていない」にフラグ変更され、出力インターフェース１８３に出力される。出力インターフェース１８３は、このデータの入力を受け、図示しない外部のビデオ記録装置にこのＰＳのデータを出力する。

【００４７】

本実施の形態では、入力ストリーム処理部１２１に入力される入力インターフェース１０１、１０３からの並列ストリームを第１暗復号演算部６０１と第２暗復号演算部６０２とで並列に復号演算するようにしている。２個の暗復号演算部６０１、６０２とを設けることで、入力された２つのストリームデータの処理を時分割処理することなく並列処理が可能となる。更に、出力ストリーム処理部６０７のクロスバスイッチ８０１のオン、オフの切換操作もストリームデータの入力される最初に１度設定しておくだけで、実施の形態１のように、調停部１５１からの経路通知毎に切換える必要がなくなる。

【００４８】

また、本実施の形態では、放送番組のＴＳとＤＶＤに記録されたＰＳとの異なる暗号アルゴリズムで暗号化されたストリームデータについて、それぞれ復号処

理をするようにしている。このような場合、１つの暗復号演算部を用いて時分割で処理するより、２個の暗復号演算部を用いる方が切り替え操作を必要とせず、処理効率が特に向上する。

【００４９】

次に、本実施の形態の動作を図９に示すフローチャートを用いて説明する。なお、図中のＳ５１２までは、上記実施の形態１と同様であるのでその説明を省略する。

Ｓ９０２において、入力ストリーム処理部１２１は、入力インターフェース１０１から入力されたＴＳパケットをＰＥＳ形式のデータに変換し、入力インターフェース１０３から入力されたＰＳパケットは無変換のＰＳ形式で、設定された第１調停部６０３又は第２調停部６０４にそれぞれ出力する（Ｓ９０４）。

【００５０】

第１調停部６０３と第２調停部６０４とは、入力されたデータと復号鍵１３１又は復号鍵１３３とを第１暗復号演算部６０１と第２暗復号演算部６０２とにそれぞれ出力する。併せて、ストリーム制御部１１１に第１暗復号演算部６０１又は第２暗復号演算部６０２にデータを出力したことを通知する（Ｓ９０６）。

ストリーム制御部１１１は、出力ストリーム制御部６０７の有するクロスバスイッチ８０１のスイッチのオン、オフを設定する（Ｓ９０８）。

【００５１】

第１暗復号演算部６０１と第２暗復号演算部６０２とは、それぞれ、入力された復号鍵１３１、１３３を用いて入力されたデータを復号演算処理して復号化したデータを出力ストリーム処理部６０７に出力する（Ｓ９１０）。

出力ストリーム処理部６０７は、入力された復号化された各データのフラグ等を変更して設定された出力インターフェース１８１、１８３に出力する（Ｓ９１２）。

【００５２】

ストリーム制御部１１１は、ＴＶ受信装置の制御部から終了指示があるか否かを判定し（Ｓ９１４）、なければＳ５０４に戻り、あれば処理を終了する。

なお、本実施の形態では、第１暗復号演算部６０１と第２暗復号演算部６０２

とを設けたけれども、入力ストリーム処理部１２１からデータが出力される経路１４１～１４４の数と同数又はそれ以上の数の暗復号演算部を設けるようにしてもよい。即ち、鍵１３１～１３４と同数の暗復号演算部を設けて、暗号化、復号化の並列処理をするようにしてもよいし、又異なる暗復号アルゴリズムの暗復号演算部を予め設けるようにしてもよい。この場合、調停部を暗復号演算部に対応して設けなければならない。

【００５３】

次に、図１０は、上記実施の形態１又は２の変形例である入力ストリーム処理部１２１のクロスバスイッチの設定状態を示している。

入力インターフェース１０２から入力される録画用の番組のＴＳストリームをＴＶ受信装置に内蔵するＨＤＤで蓄積するとともに、外部のビデオ録画装置でも記録するように、出力インターフェース１８２、１８３に出力するため、入力ストリーム処理部１２１は、ＰＥＳ形式に変換されたデータを経路１４２、１４３とに出力する。

【００５４】

ストリーム制御部１１１は、クロスバスイッチ１００１の接点１００２、１００３とをオンに設定している。

また、別の変形例として、入力インターフェース１０２から２チャネルの番組のＴＳストリームが入力されている場合、ストリーム解析部１１０で各チャネルに対応するＰＩＤをストリーム制御部１１１に通知する。ストリーム制御部１１１は、接点１００２、１００３とを２個のＰＩＤに応じてオン、オフを制御する。これによって、経路１４２には１のチャネルの番組のＰＥＳパケットを、経路１４３には他のチャネルの番組のＰＥＳパケットをそれぞれ出力することになる。入力ストリーム処理部１２１は、デマルチプレクス処理をすることになる。

【００５５】

図１１は、更に他の変形例である入力ストリーム処理部１２１のクロスバスイッチの設定状態を示している。

クロスバスイッチ１１０１の接点１１０２、１１０３がオンに設定されている。

入力インタフェース１０１には、有る番組に一定時間毎にあるＣＭの挿入されたＴＳストリームが入力されている。入力インターフェース１０２には、別の番組に一定時間毎に別のＣＭの挿入されたＴＳストリームが入力されている。

【００５６】

ストリーム制御部１１１は、入力インターフェース１０１にある番組のＴＳパケットの出力指示とあるＣＭのＴＳパケットの廃棄指示とをし、入力インターフェース１０２に別の番組のＴＳパケットの廃棄指示と別のＣＭのＴＳパケットの出力指示とをする。

入力ストリーム処理部１２１では、２つのＴＳストリームを１つのＴＳストリームにするマルチプレクス処理が行われる。即ち、経路１４２には、ある番組のＴＳパケットと別のＣＭのＴＳパケットが１つのＴＳストリームとして出力される。

【００５７】

なお、図１０、図１１では、入力ストリーム処理部１２１でのデマルチプレクス処理と、マルチプレクス処理とを説明したけれども、出力ストリーム処理部１７１等でデマルチプレクス処理とマルチプレクス処理とが行われるようにしてもよいのは勿論である。

（実施の形態３）

図１２は、本発明に係る並列ストリーム暗復号装置の実施の形態３の構成図である。

【００５８】

この並列ストリーム暗復号装置は、上述した実施の形態１のそれと、入力ストリーム処理部１２０１と調停部１５１との間の経路１２１１～１２１４に分岐経路１２２１～１２２４をそれぞれ設け、分岐経路１２２１～１２２４を出力ストリーム処理部１２０３にそれぞれ接続していることと、暗復号演算部１６１と出力ストリーム処理部１２０３との間の経路１２３１に分岐経路１２４１を設け、分岐経路１２４１を入力インターフェース１０５に接続していることとが異なるだけである。

【００５９】

以下、本実施の形態固有の構成についてのみ説明する。

本実施の形態では、暗号化された番組のＴＳの入力を入力インターフェース１０１が受け、この番組を視聴するとともに、暗号化された状態の番組を内蔵のＨＤＤに記録し、更に、一旦復号化した番組を別の暗号鍵で暗号化して外部のビデオ記録装置に記録する。

【００６０】

出力インターフェース１８１は、ＴＶ受信装置の表示部に復号化されたデータを出力し、出力インターフェース１８２は、ＨＤＤに暗号化されたままのデータを出力し、出力インターフェース１８３は、再暗号化したデータを外部のビデオ記録装置に出力する。

図１３は、入力ストリーム処理部１２０１のクロスバスイッチの設定状態を示している。クロスバスイッチ１３０１の接点１３０２、１３０３がオンに設定されている。

【００６１】

入力インターフェース１０１は、番組のＴＳ入力を受け、ストリーム制御部１１１の出力指示により、入力ストリーム処理部１２０１にＴＳパケットを出力する。入力ストリーム処理部１２０１は、入力されたＴＳパケットをＰＥＳ形式のパケットに変換する。ＰＥＳ形式のパケットは、クロスバスイッチ１３０１を経由して、経路１２１１、１２２１に出力される。経路１２２１に出力されたデータは、出力ストリーム処理部１２０３に直接入力される。経路１２１１に出力されたＰＥＳ形式のパケットは、調停部１５１に出力される。

【００６２】

調停部１５１は、入力されたＰＥＳ形式のパケットと復号鍵１３１とを暗復号演算部１６１に出力し、ストリーム制御部１１１に経路１２１１から入力されたデータを暗復号演算部１６１に出力したとことを通知する。

暗復号演算部１６１は、入力されたデータを復号鍵１３１で復号化し、復号したデータを経路１２３１、１２４１に出力する。経路１２３１に出力された復号化されたデータは、出力ストリーム処理部１２０３に入力される。

【００６３】

経路１２４１に出力された復号化されたデータは、入力インターフェース１０５に入力される。ストリーム制御部１１１は、入力インターフェース１０５に入力されたデータが経路１２１１を経由したデータであるとき、入力ストリーム処理部１２０１への出力指示をする。

なお、経路１２１３を経由したデータが経路１２４１から入力インターフェース１０５に入力されたときには、ストリーム制御部１１１は、そのデータの廃棄を指示する。

入力ストリーム処理部１２０１は、入力インターフェース１０５から入力された復号化されたデータを無変換でクロスバスイッチ１３０１を経由して、経路１２１３、１２２３に出力する。ここで、無変換としているのは、このデータが既にＰＥＳ形式のパケットに変換されているからである。

【００６４】

経路１２２３に出力された復号化されたデータは、出力ストリーム処理部１２０３に入力される。

経路１２１３に出力されたデータは、調停部１５１に入力される。調停部１５１は、このデータと暗号鍵１３３とを暗復号演算部１６１に出力するとともに、ストリーム制御部１１１に経路１２１３から入力されたデータを暗復号演算部１６１に出力したことを通知する。

【００６５】

暗復号演算部１６１は、暗号鍵１３３を用いてデータを暗号化し、暗号化したデータを経路１２３１、１２４１に出力する。経路１２３１に出力された暗号化されたデータは、出力ストリーム処理部１２０３に入力され、経路１２４１に出力された暗号化されたデータは再び入力インターフェース１０５に入力される。なお、この暗号化されたデータは、上述のように入力インターフェース１０５によってストリーム制御部１１１の指示により廃棄される。

【００６６】

図１４、図１５は、出力ストリーム処理部１２０３のクロスバスイッチの設定状態を示す図である。図１４では、クロスバスイッチ１４０１の接点１４０２、１４０３がオンに設定されている。

出力ストリーム処理部１２０３は、経路１２２１から入力される暗号化されたデータの番組情報を変更して出力インターフェース１８２に出力する。

【００６７】

また、経路１２３１から入力される経路１２１１を経由した復号化されたデータを番組情報と、「スクランブルがかかっていない」のフラグとに変更して出力インターフェース１８１に出力する。

次に、出力ストリーム処理部１２０３に経路１２３１から入力される経路１２１３を経由した再暗号化されたデータが入力されたとき、ストリーム制御部１１１によって、図１５に示すように、クロスバスイッチ１４０１の接点１４０３がオフにされ接点１５０１がオンにされる。これによって、再暗号化されたデータは、番組情報が変更され、出力インターフェース１８３に出力される。

【００６８】

なお、経路１２２３から入力されるデータは、クロスバスイッチ１４０１の接点が全てオフ状態であるので、出力インターフェースに出力されることはない。

また、復号鍵１３１や暗号鍵１３３は、ＴＶ受信装置の制御部によって設定され、ストリーム制御部１１１に通知される。

本実施の形態において、外部のビデオ記録装置に出力する出力インターフェース１８３へのデータを再暗号化したのは、著作権を保護するためである。

【００６９】

本実施の形態の動作は、本質的に実施の形態１のそれと異なるものではないので説明を省略する。

なお、上記各実施の形態において、鍵１３１～１３４は、入力インターフェース１０１～１０５から入力されるストリームデータに応じてＴＶ受信装置の制御部において予め設定される。この鍵は、例えば、ＴＶ受信装置に挿入されたカードや受信されたストリームデータ中に記録されているものである。

【００７０】

上記各実施の形態の構成図を図１、図６、図１２に示したけれども、各構成要素の機能をコンピュータに発揮させるプログラムで実現するようにしてもよい。このプログラムをコンピュータ読み取り可能な記録媒体に記録して並列ストリー

ム暗復号装置に適用してもよいし、インターネット上のサイトに記録しておき、ダウンロードさせて並列ストリーム暗復号装置に適用してもよい。

【００７１】

【発明の効果】

以上説明したように、本発明は、ストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路と、入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理手段と、出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算手段とを備えることとしている。このような構成によって、暗復号演算手段は、ストリームデータの入力される経路に対応した鍵を用いて暗号化又は復号化することができるので、ストリームデータに応じていちいち鍵を選択する必要がなくなり、制御手順が簡略化される。

【００７２】

また、前記入力ストリーム処理手段は、クロスバスイッチを有し、ストリームデータの入力線とストリームデータを暗号化又は復号化する鍵に対応する経路に接続される出力線との接点のスイッチをオンに設定することにより、対応する経路にストリームデータを出力することとしている。このような構成によって、ストリームデータに対応した鍵の設定された経路に容易にストリームデータを出力することができる。

【００７３】

また、前記暗復号演算手段で暗号化又は復号化された複数のストリームデータの入力を受け、複数の出力インターフェースに各暗号化又は復号化されたストリームデータをそれぞれ出力する出力ストリーム処理手段を更に備えることとしている。このような構成によって、暗号化又は復号化されたストリームデータを適切な出力インターフェースに出力することができる。

【００７４】

また、前記出力ストリーム処理手段は、クロスバスイッチを有し、前記出力ストリーム処理手段から出力される複数の暗号化又は復号化されたストリームデータの出力先の出力インターフェースを前記経路に応じてクロスバスイッチをオン

オフ制御して切り換える制御手段と、複数の経路へ出力されたストリームデータと対応する鍵とを前記暗復号演算手段に経路毎に入力し、入力したストリームデータの経路情報を前記制御手段に通知する入力通知手段を更に備えることとしている。このような構成によって、ストリームデータを暗号化又は復号化したストリームデータの出力先の出力インターフェースを容易に設定することができる。

【００７５】

また、前記暗復号演算手段を複数備え、前記複数の経路へ出力されるストリームデータと対応する鍵とを各暗復号演算手段に並列入力し、各暗復号演算手段に入力したストリームデータの経路情報を通知する入力通知手段と、前記経路情報に従い、前記出力ストリーム処理手段から出力される複数の暗号化又は復号化されたストリームデータの出力先の出力インターフェースを選択制御する制御手段とを更に備えることとしている。このような構成によって、暗号化又は復号化を並列処理することができるので、暗号化又は復号化のスループットが向上する。

【００７６】

また、前記暗復号演算手段から出力された暗号化又は復号化されたストリームデータを再度前記入力ストリーム処理手段に入力する経路を更に備え、前記暗復号演算手段は、暗号化又は復号化されたストリームデータを異なる鍵で暗号化又は復号化することとしている。このような構成によって、例えば、暗号化又は復号化されたストリームデータを異なる暗号鍵によって再暗号化することができるので、著作権等の保護の実効を強化できる。

【００７７】

また、前記入力ストリーム処理手段は、入力される複数のストリームデータをマルチプレクス処理して１つのストリームデータを生成することとしている。このような構成によって並列して入力される複数のストリームデータから新たなストリームデータを生成した後、暗号化又は復号化をすることができる。

また、前記入力ストリーム処理手段は、入力される１つのストリームデータをデマルチプレクス処理して複数のストリームデータを生成することとしている。このような構成によって、例えば、複数の番組が多重化されたストリームデータの入力を受け、個々の番組のストリームデータに分離することができる。

【００７８】

また、前記入力ストリーム処理手段は、入力される１つのストリームデータを２つの経路に出力し、１つの経路は、前記暗復号演算手段に、別の経路は、直接前記出力ストリーム処理手段にそれぞれ接続されていることとしている。このような構成によって、暗号化又は復号化を要しないストリームデータもいっしょに入力ストリーム処理手段に入力することができる。

【００７９】

また、ストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路を備える並列ストリーム暗復号装置における並列ストリーム暗復号方法であって、入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理ステップと、出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算ステップとを有することとしている。このような方法によって、暗復号演算ステップにおいて、入力されるストリームデータに応じて鍵をいちいち選択する煩雑な操作の必要がなくなる。

【００８０】

また、上記並列ストリーム暗復号方法をコンピュータに実行させるプログラムとしている。このようなプログラムをストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する経路を有する並列ストリーム暗復号装置に適用して、暗号化又は復号化する鍵をいちいち選択する煩雑な操作を回避することができる。

【００８１】

更に、上記並列ストリーム暗復号装置を組み込んだＴＶ受信装置としている。このような構成によって、ＴＶ受信装置は、効率的に受信したストリームデータの暗号化又は復号化をすることが可能となる。

【図面の簡単な説明】

【図１】　本発明にかかる並列ストリーム暗復号装置の実施の形態１の構成図である。

【図２】　上記実施の形態の入力ストリーム処理部のクロスバスイッチのスイッチの状態を示す図である。

【図３】　上記実施の形態の出力ストリーム処理部のクロスバスイッチのスイッチの状態の一例を示す図である。

【図４】　上記実施の形態の出力ストリーム処理部のクロスバスイッチのスイッチの状態の他の例を示す図である。

【図５】　上記実施の形態の動作を説明するフローチャートである。

【図６】　本発明に係る並列ストリーム暗復号装置の実施の形態２の構成図である。

【図７】　上記実施の形態の入力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図８】　上記実施の形態の出力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図９】　上記実施の形態の動作を説明するフローチャートである。

【図１０】上記実施の形態の変形例の入力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図１１】上記各実施の形態の別の変形例の入力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図１２】本発明に係る並列ストリーム暗復号装置の実施の形態３の構成図である。

【図１３】上記実施の形態の入力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図１４】上記実施の形態の出力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図１５】上記実施の形態の出力ストリーム処理部のクロスバスイッチの設定状態の他の例を示す図である。

【図１６】従来の並列ストリーム暗復号装置の構成図である。

【符号の説明】

１０１～１０５	入力インターフェース
１１０	ストリーム解析部
１１１	ストリーム制御部

１２１，１２０１　入力ストリーム処理部

１３１～１３４　鍵

１４１～１４４，１２１１～１２１４，１２２１～１２２４　経路

１５１　調停部

１６１　暗復号演算部

１７１，６０７，１２０３　出力ストリーム処理部

１８１～１８５　出力インターフェース

２０１，３０１，７０１，８０１，１００１，１１０１，１３０１，１４０１　クロスバスイッチ

６０１　第１暗復号演算部

６０２　第２暗復号演算部

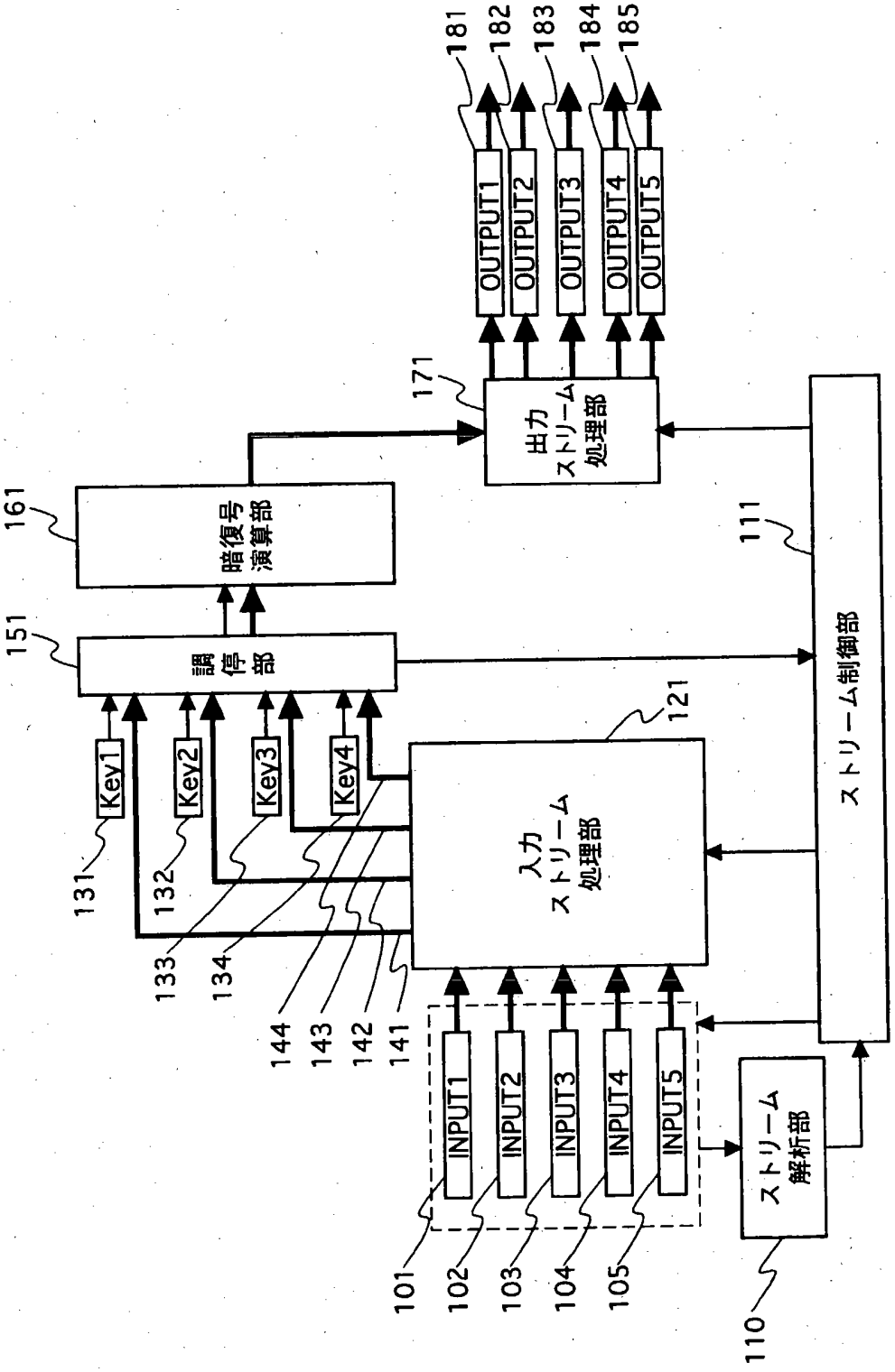
６０３　第１調停部

６０４　第２調停部

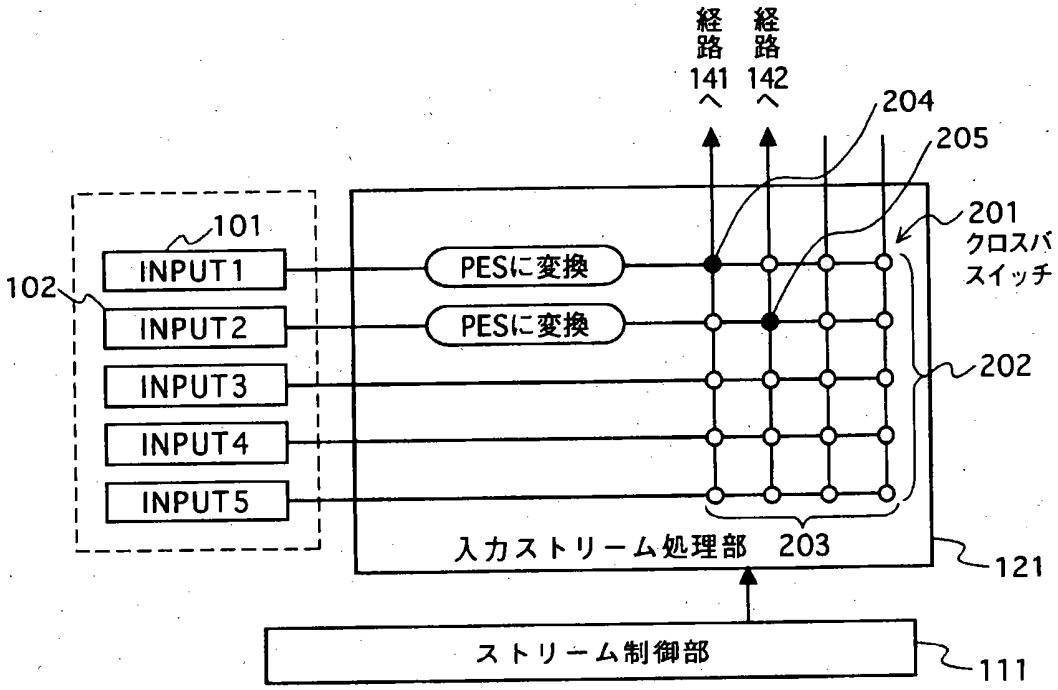
６０６，６０７，１２３１，１２４１　経路

【書類名】　　図面

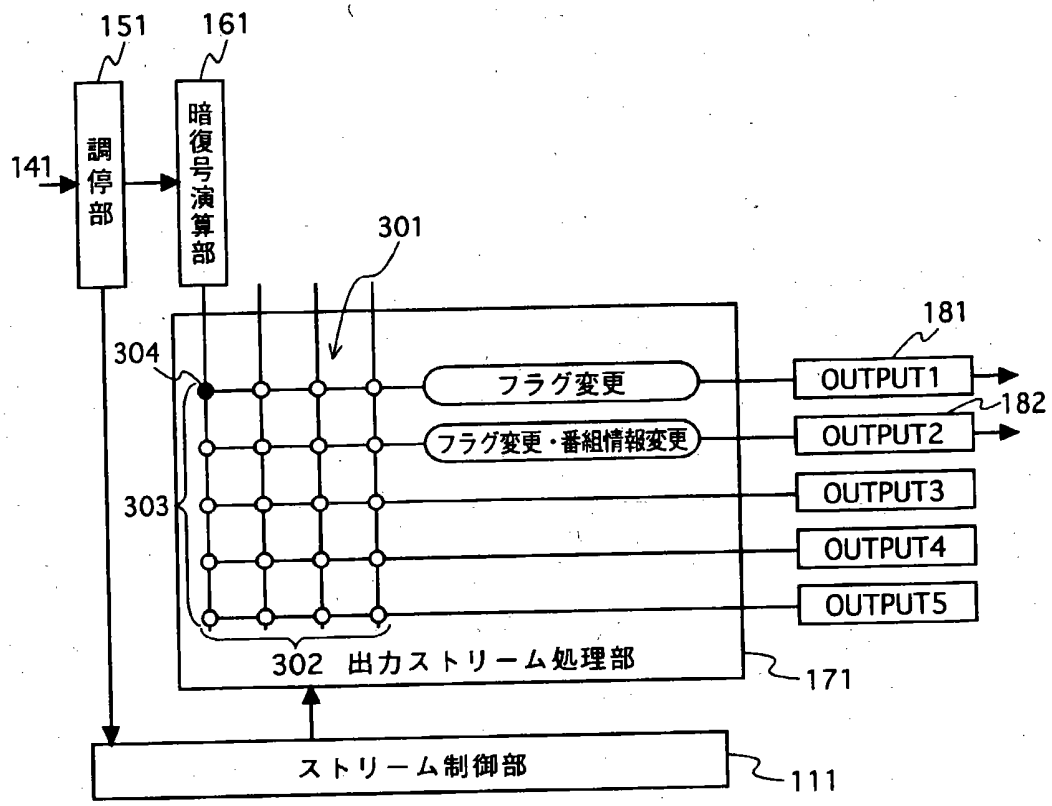
【図１】


181
182
183
184
185
OUTPUT1
OUTPUT2
OUTPUT3
OUTPUT4
OUTPUT5
171
出力ストリーム処理部
161
暗復号演算部
111
ストリーム制御部
151
調停部
121
Key1
Key2
Key3
Key4
入力ストリーム処理部
131
132
133
134
144
143
142
141
INPUT1
INPUT2
INPUT3
INPUT4
INPUT5
ストリーム解析部
101
102
103
104
105
110

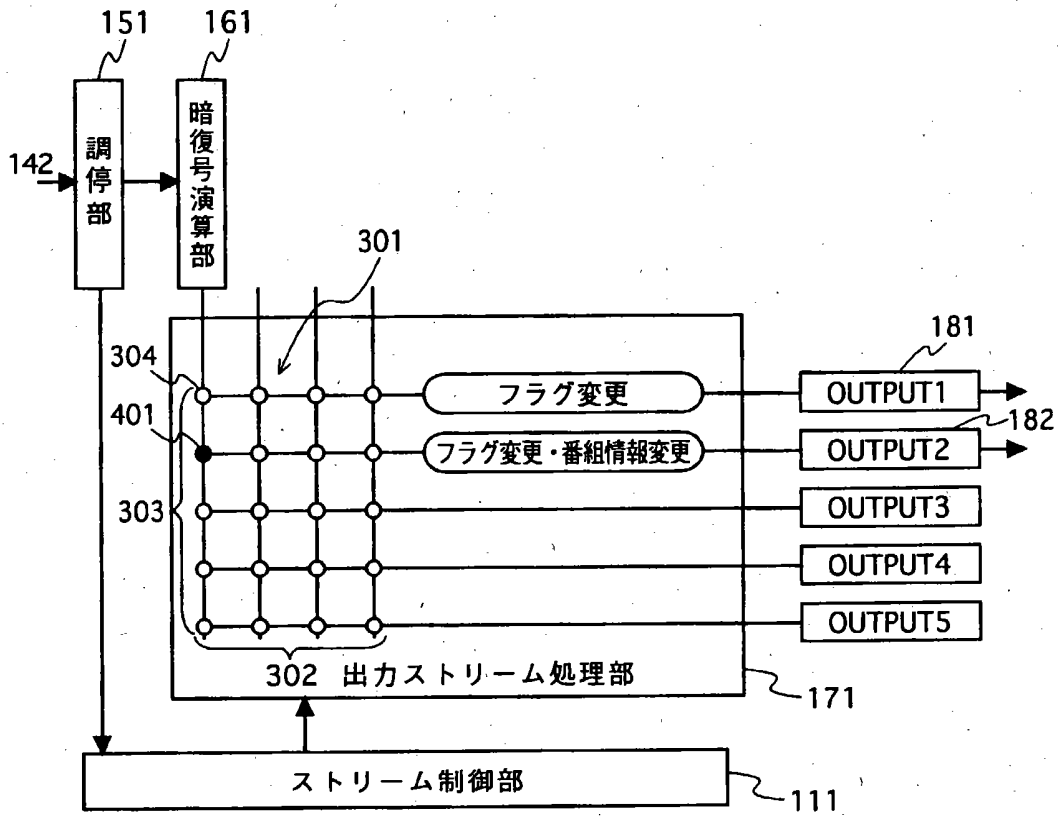
【図２】


経路141へ
経路142へ
204
205
201
クロスバスイッチ
101
102
INPUT1
INPUT2
INPUT3
INPUT4
INPUT5
PESに変換
PESに変換
202
入力ストリーム処理部　203
121
ストリーム制御部
111

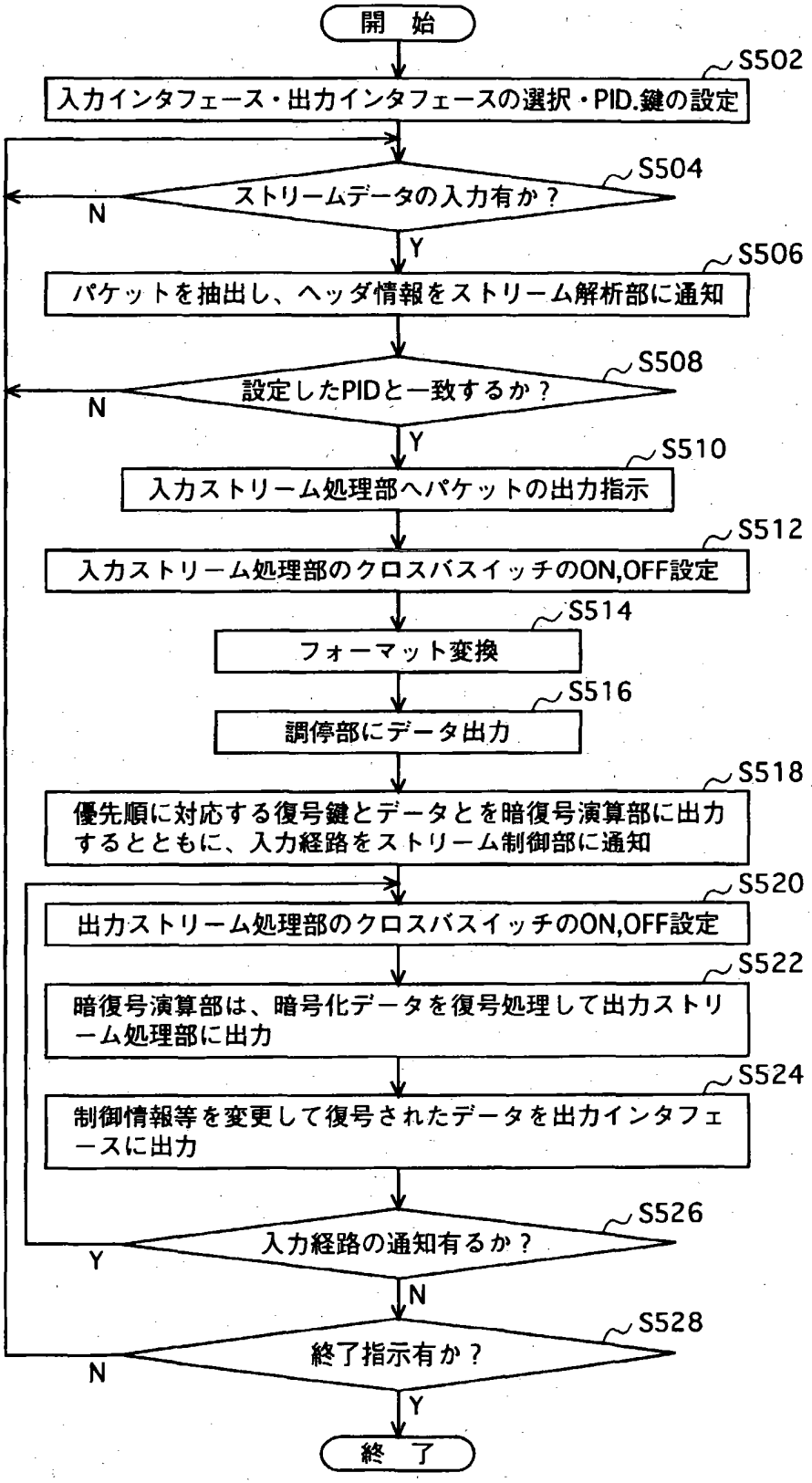
【図３】


151
161
141
調停部
暗復号演算部
301
304
303
181
フラグ変更
フラグ変更・番組情報変更
OUTPUT1
OUTPUT2
182
OUTPUT3
OUTPUT4
OUTPUT5
302 出力ストリーム処理部
171
ストリーム制御部
111

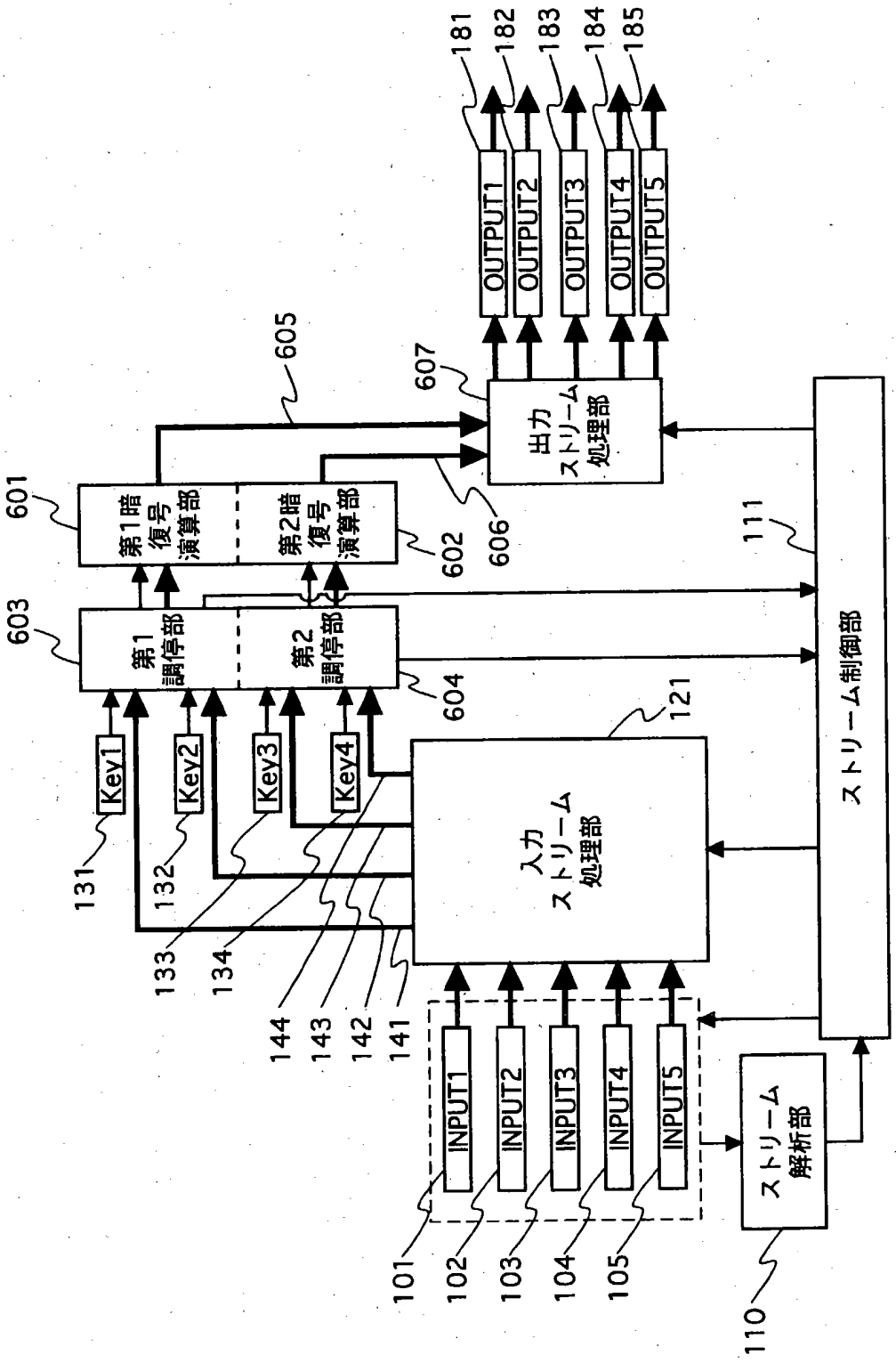
【図４】


151
161
142
調停部
暗復号演算部
301
304
401
303
181
フラグ変更
フラグ変更・番組情報変更
OUTPUT1
OUTPUT2
182
OUTPUT3
OUTPUT4
OUTPUT5
302 出力ストリーム処理部
171
ストリーム制御部
111

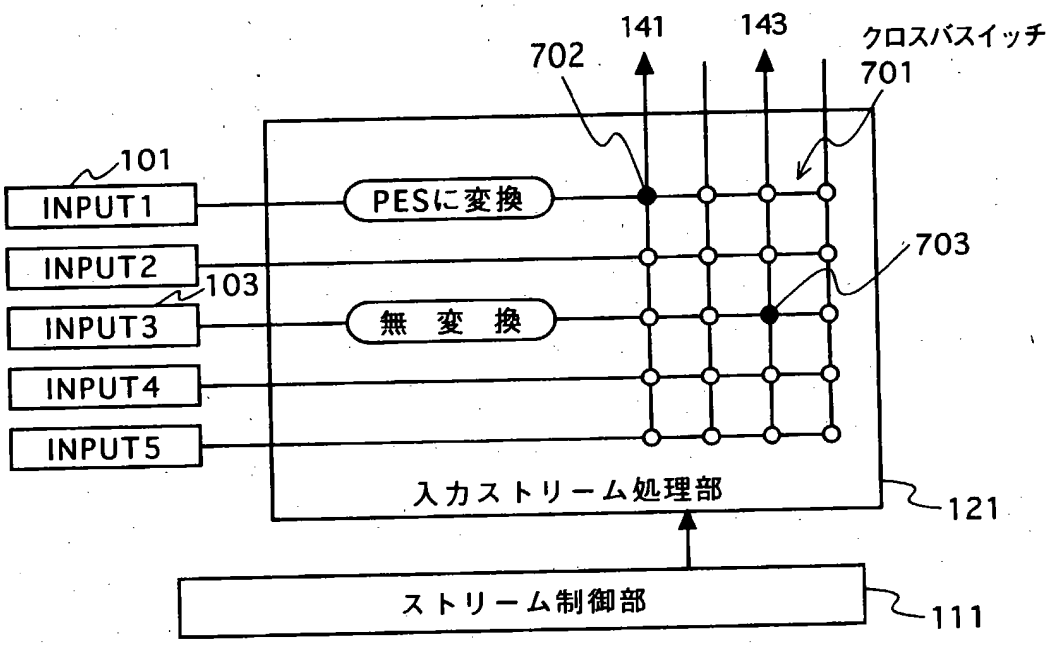
【図５】


開　始
S502
入力インタフェース・出力インタフェースの選択・PID.鍵の設定
S504
ストリームデータの入力有か？
N
Y
S506
パケットを抽出し、ヘッダ情報をストリーム解析部に通知
S508
設定したPIDと一致するか？
N
Y
S510
入力ストリーム処理部へパケットの出力指示
S512
入力ストリーム処理部のクロスバスイッチのON,OFF設定
S514
フォーマット変換
S516
調停部にデータ出力
S518
優先順に対応する復号鍵とデータとを暗復号演算部に出力するとともに、入力経路をストリーム制御部に通知
S520
出力ストリーム処理部のクロスバスイッチのON,OFF設定
S522
暗復号演算部は、暗号化データを復号処理して出力ストリーム処理部に出力
S524
制御情報等を変更して復号されたデータを出力インタフェースに出力
S526
入力経路の通知有るか？
Y
N
S528
終了指示有か？
N
Y
終　了

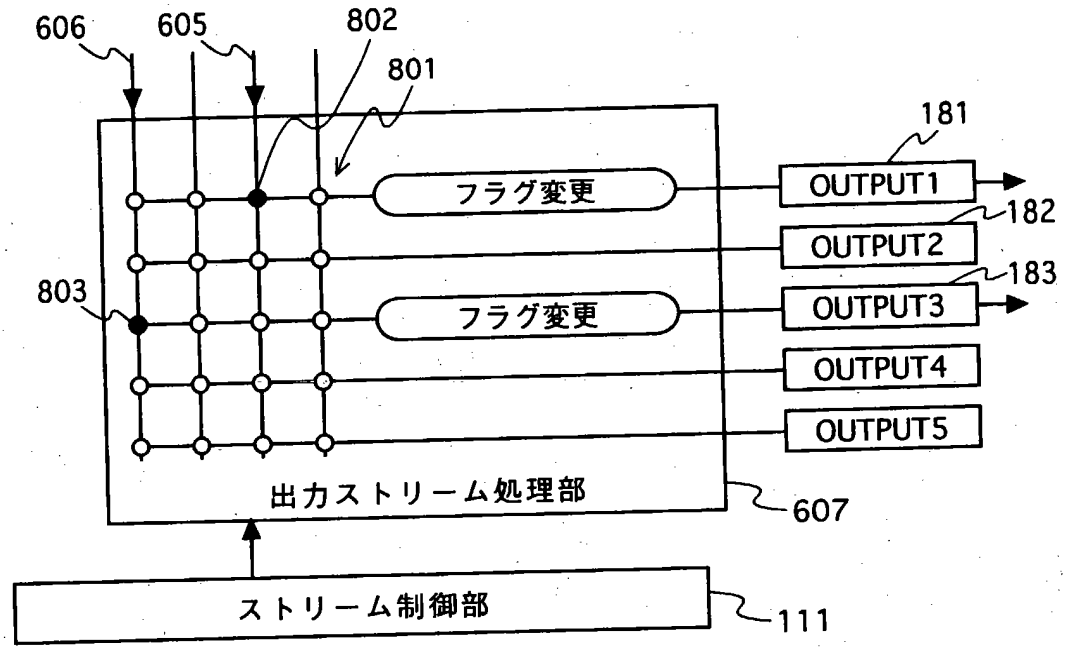
【図６】


181
182
183
184
185
OUTPUT1
OUTPUT2
OUTPUT3
OUTPUT4
OUTPUT5
605
607
出力
ストリーム
処理部
601
第1暗
復号
演算部
第2暗
復号
演算部
602
606
111
603
第1
調停部
第2
調停部
604
121
Key1
Key2
Key3
Key4
入力
ストリーム
処理部
ストリーム制御部
131
132
133
134
144
143
142
141
INPUT1
INPUT2
INPUT3
INPUT4
INPUT5
ストリーム
解析部
101
102
103
104
105
110

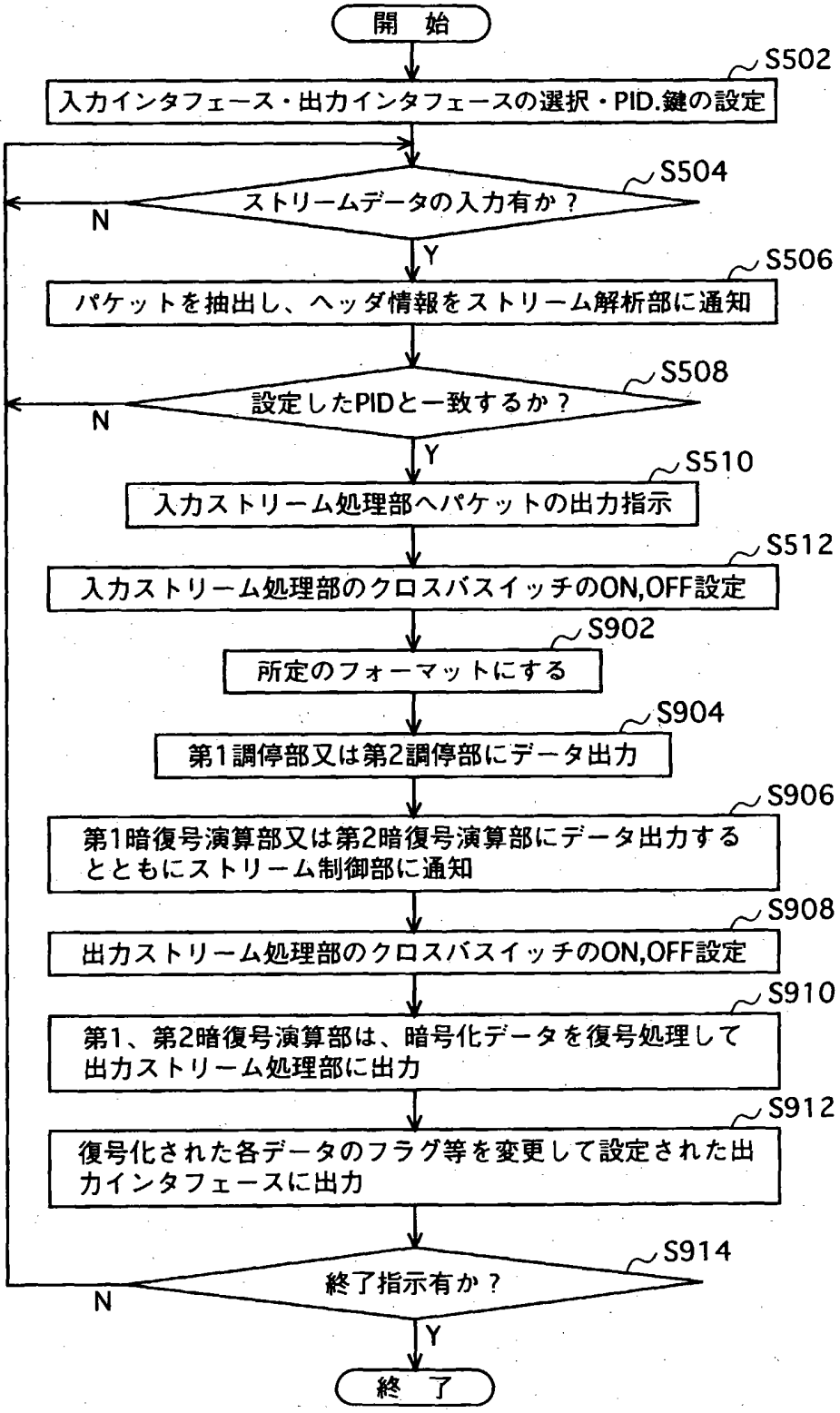
【図７】


141
143
クロスバスイッチ
702
701
101
INPUT1
PESに変換
INPUT2
703
103
INPUT3
無　変　換
INPUT4
INPUT5
入力ストリーム処理部
121
ストリーム制御部
111

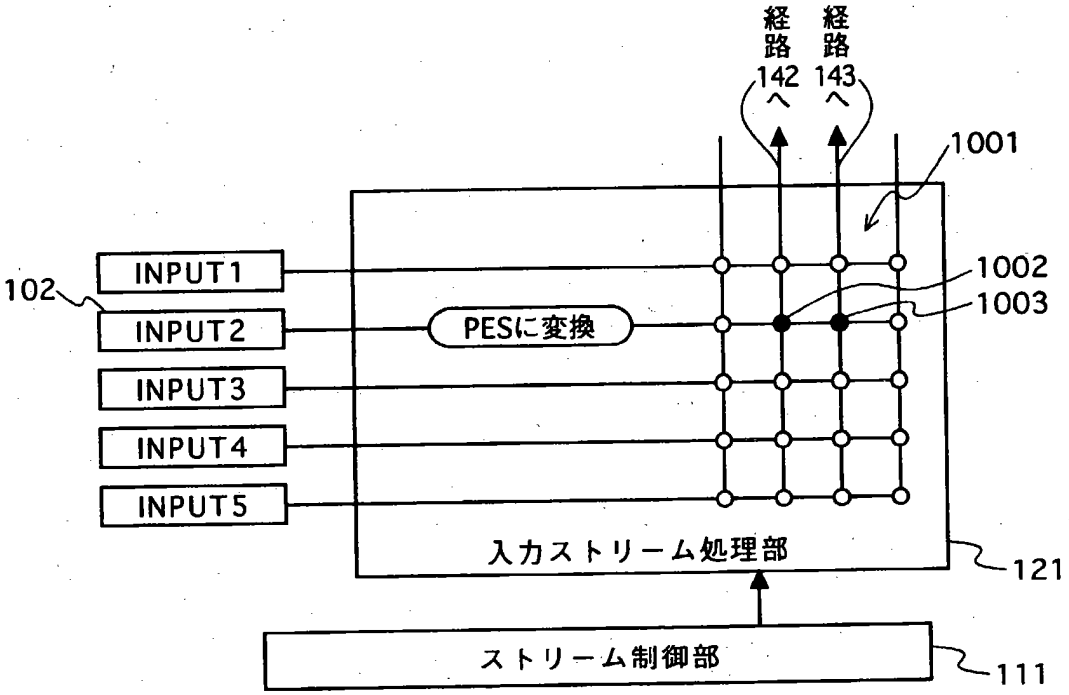
【図８】


606
605
802
801
181
フラグ変更
OUTPUT1
182
OUTPUT2
183
803
フラグ変更
OUTPUT3
OUTPUT4
OUTPUT5
出力ストリーム処理部
607
ストリーム制御部
111

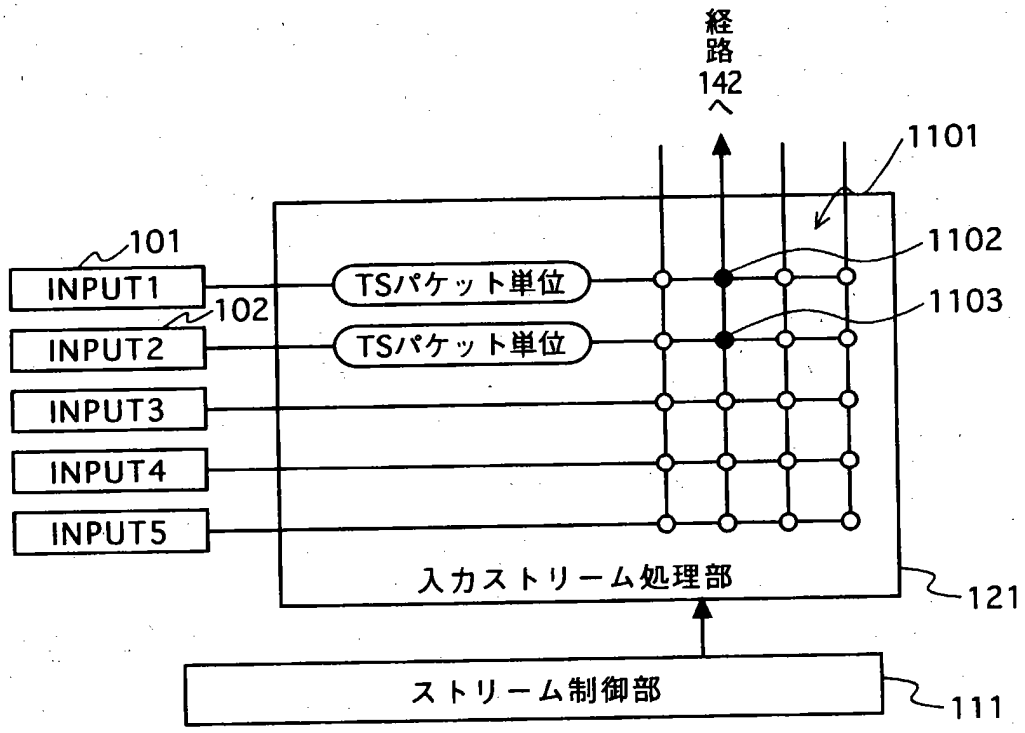
【図９】


開　始
S502
入力インタフェース・出力インタフェースの選択・PID.鍵の設定
S504
ストリームデータの入力有か？
N
Y
S506
パケットを抽出し、ヘッダ情報をストリーム解析部に通知
S508
設定したPIDと一致するか？
N
Y
S510
入力ストリーム処理部へパケットの出力指示
S512
入力ストリーム処理部のクロスバスイッチのON,OFF設定
S902
所定のフォーマットにする
S904
第1調停部又は第2調停部にデータ出力
S906
第1暗復号演算部又は第2暗復号演算部にデータ出力するとともにストリーム制御部に通知
S908
出力ストリーム処理部のクロスバスイッチのON,OFF設定
S910
第1、第2暗復号演算部は、暗号化データを復号処理して出力ストリーム処理部に出力
S912
復号化された各データのフラグ等を変更して設定された出力インタフェースに出力
S914
終了指示有か？
N
Y
終　了

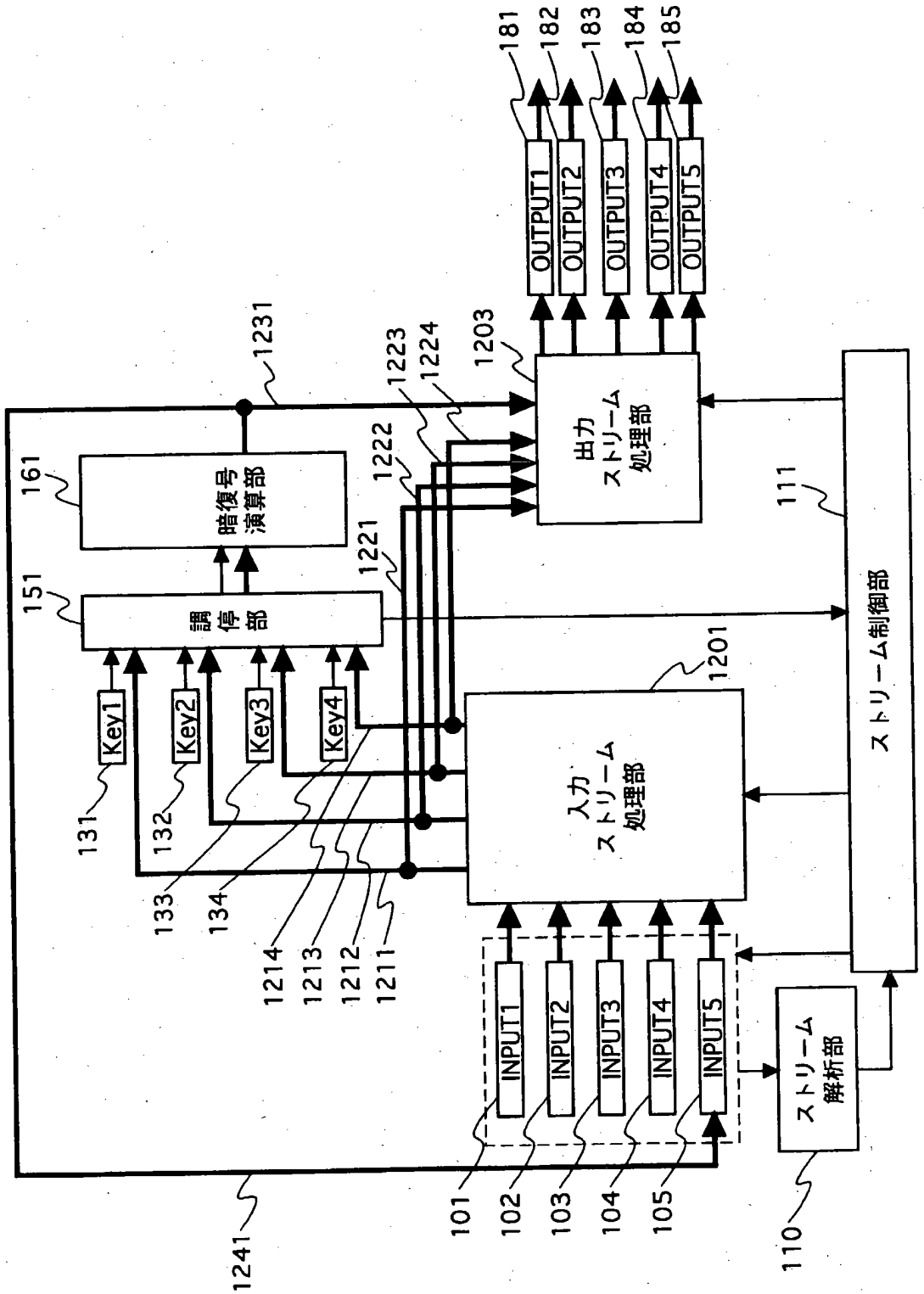
【図１０】


経路142へ
経路143へ
1001
1002
1003
102
INPUT1
INPUT2
INPUT3
INPUT4
INPUT5
PESに変換
入力ストリーム処理部
121
ストリーム制御部
111

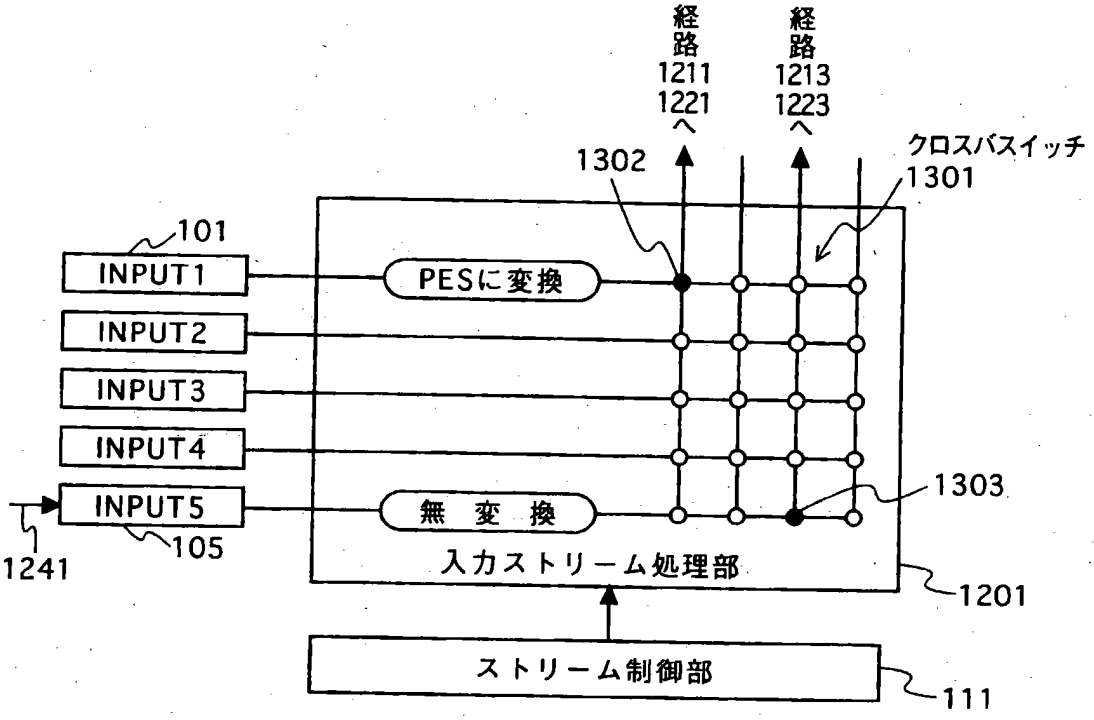
【図１１】


経路
142
へ
1101
101
INPUT1
102
INPUT2
INPUT3
INPUT4
INPUT5
TSパケット単位
TSパケット単位
1102
1103
入力ストリーム処理部
121
ストリーム制御部
111

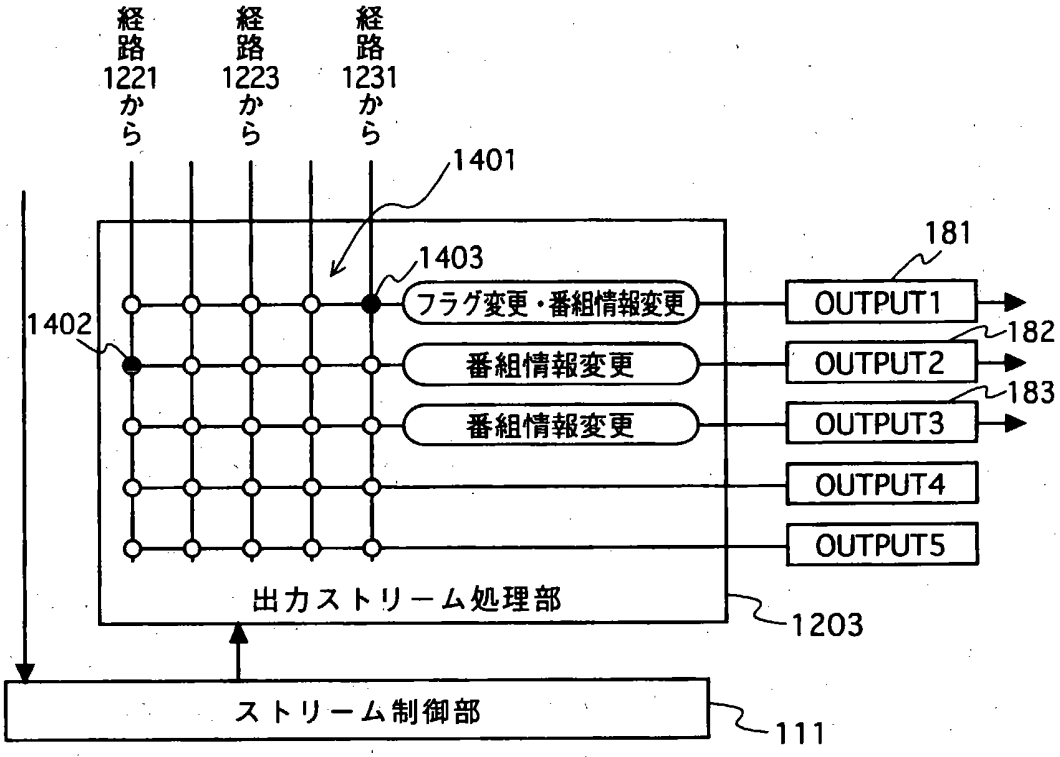
【図１２】


181
182
183
184
185
OUTPUT1
OUTPUT2
OUTPUT3
OUTPUT4
OUTPUT5
1231
1223
1224
1203
出力
ストリーム
処理部
161
暗復号
演算部
1222
1221
111
151
調停部
ストリーム制御部
1201
Key1
Key2
Key3
Key4
入力
ストリーム
処理部
131
132
133
134
1214
1213
1212
1211
INPUT1
INPUT2
INPUT3
INPUT4
INPUT5
ストリーム
解析部
1241
101
102
103
104
105
110

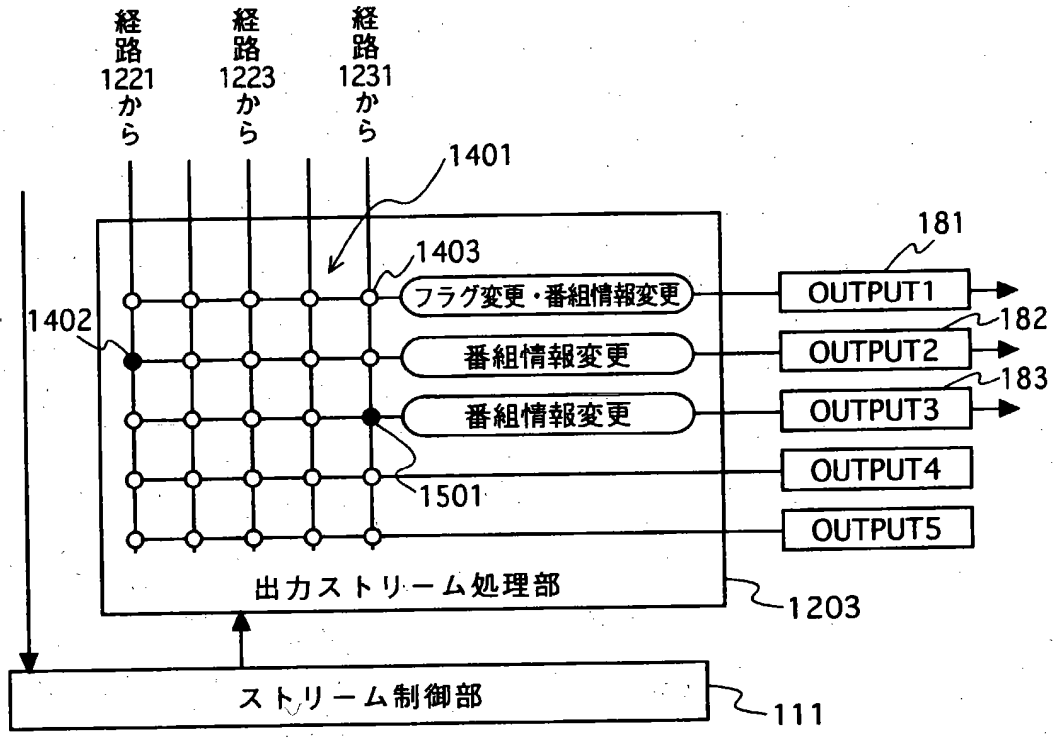
【図１３】


経路
1211
1221
へ
経路
1213
1223
へ
クロスバスイッチ
1301
1302
101
INPUT1
PESに変換
INPUT2
INPUT3
INPUT4
INPUT5
無　変　換
1303
1241
105
入力ストリーム処理部
1201
ストリーム制御部
111

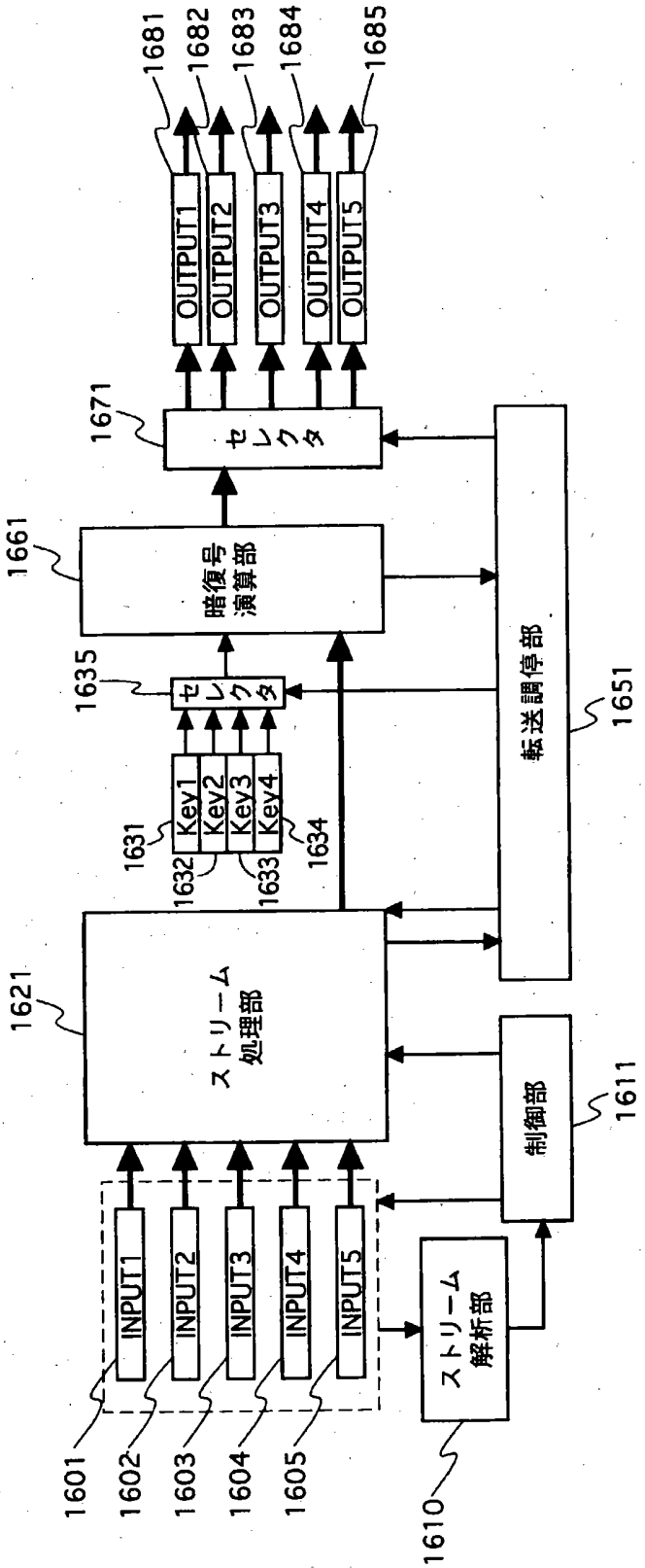
【図１４】


経路1221から
経路1223から
経路1231から
1401
1403
1402
181
フラグ変更・番組情報変更
番組情報変更
番組情報変更
OUTPUT1
OUTPUT2
OUTPUT3
OUTPUT4
OUTPUT5
182
183
出力ストリーム処理部
1203
ストリーム制御部
111

【図１５】


経路1221から
経路1223から
経路1231から
1401
1403
1402
フラグ変更・番組情報変更
番組情報変更
番組情報変更
1501
出力ストリーム処理部
1203
ストリーム制御部
111
181
OUTPUT1
182
OUTPUT2
183
OUTPUT3
OUTPUT4
OUTPUT5

【図１６】


1681
1682
1683
1684
1685
OUTPUT1
OUTPUT2
OUTPUT3
OUTPUT4
OUTPUT5
1671
セレクタ
1661
暗復号演算部
1635
セレクタ
1631
Key1
Key2
Key3
Key4
1632
1633
1634
1621
ストリーム処理部
転送調停部
1651
制御部
1611
INPUT1
INPUT2
INPUT3
INPUT4
INPUT5
ストリーム解析部
1601
1602
1603
1604
1605
1610

【書類名】　要約書

【要約】

【課題】　並列入力されるストリームデータを鍵を用いて暗号化又は復号化する並列ストリーム暗復号装置のストリームデータに対応する鍵の選択の煩雑さを回避する。

【解決手段】　ストリームデータを暗号化等する複数の鍵１３１～１３４に対応する経路１４１～１４４を設けている。入力インターフェース１０１から入力されるＴＳは、復号鍵１３１で、入力インターフェース１０２から入力されるＴＳは、復号鍵１３２で復号される。入力ストリーム処理部１２１は、入力インターフェース１０１から入力されたＴＳデータを復号鍵１３１に対応する経路１４１に、入力インターフェース１０２から入力されたＴＳデータを復号鍵１３２に対応する経路１４２に出力する。暗復号演算部１６１は、経路１４１から入力されたＴＳデータを復号鍵１３１で、経路１４２から入力されたＴＳデータを復号鍵１３２でそれぞれ復号する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社